Amendments to the Claims:

1. (Currently Amended) A network switch comprising;
   a memory for storing a first secret fact;
   a port for sending said secret fact to a second switch;
   a port for receiving,
      a second-type derivative of said first secret fact from said second switch,
      pre-defined information about said second switch, and
      a third-type derivative of said pre-defined information about said second switch, the third-type derivative of said pre-defined information about said second switch being generated by the second switch;
   a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch.

2. (Previously Presented) The switch of claim 1 wherein said port for sending said secret fact to a second switch and said port for receiving, a second-type derivative of said first secret fact from said second switch, pre-defined information about said second switch, and a third-type derivative of said pre-defined information about said second switch are the same port.

3. (Previously Presented) The switch of claim 1 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes reversing the derivation resulting in said second-type derivative to recreate said first secret fact.

4. (Original) The switch of claim 1 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes creating a second-type derivative of said first secret fact.

5. (Previously Presented) The network switch of claim 1 wherein said second-type derivative is specific to said second switch.

6. (Previously Presented) The network switch of claim 1 wherein said third-type derivative is specific to said first switch and said second switch.

7. (Original) The network switch of claim 1 wherein said pre-defined information about said second switch comprises encryption key information.

8. (Original) The network switch of claim 1 wherein said first secret fact is a random number.

9. (Original) The network switch of claim 1 wherein said first secret fact is a nonce.

10. (Currently Amended) A method of mutually authenticating a first port on a first switch with a second port on a second switch, said first port coupled to said second port by a communication medium that is exclusive to said first port and said second port, the method comprising the steps of:

sending a first fact from said first port to said second port;

at said second switch,

creating a second-type derivative of said first fact,

sending said second-type derivative of said first fact from said second port to said first port;

at said first switch,

storing said second-type derivative of said first fact in a first memory;

sending a second fact from said second port to said first port;

at said first switch, creating a first-type derivative of said second fact;

sending said first-type derivative of said second fact from said first port to said second port;

at said second switch, storing said first-type derivative of said second fact in a second memory;

sending defined information concerning said first switch from said first port to said second port;

sending a third-type derivative of said defined information concerning said first switch from said first port to said second port, the third-type derivative of said defined information concerning said first switch being generated by the first switch;

at said second switch, comparing said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch;

at said second switch, comparing said first type derivative of said second fact with said second fact;

sending defined information concerning said second switch from said second port to said first port;

sending a third-type derivative of said defined information concerning said second switch from said second port to said first port, the third-type derivative of said defined information concerning said second switch being generated by the second switch;

at said first switch, comparing said defined information concerning said second switch with said third-type derivative of said defined information concerning said second switch; and

at said first switch, comparing said second type derivative of said first fact with said first fact.

11. (Original) The method of claim 10 wherein the step of comparing said defined information concerning said second switch with said third-type derivative of said defined information concerning said second switch, comprises the substeps of:

reversing the derivation of the third-type derivative of said defined information concerning said second switch; and

comparing the result of said reversal with said defined information concerning said second switch.

12. (Original) The method of claim 10 wherein the step of comparing said defined information concerning said second switch with said third-type derivative of said defined information concerning said second switch, comprises the substeps of:

making a third-type derivative of said defined information concerning said second switch; and

comparing the made third-type derivative with the received third-type derivative.

13. (Original) The method of claim 10 wherein the step, at said second switch, of creating a second-type derivative of said first fact comprises the sub-steps of:

encoding said first fact to yield an encoded first fact; and

encrypting said encoded first fact.

14. (Original) The method of claim 13 wherein said encoding is performed by applying a hash function.

15. (Original) The method of claim 13 wherein said encrypting is performed using a private key unique to said second switch.

16. (Original) The method of claim 10 wherein said defined information concerning said first switch comprises encryption key information.

17. (Original) The method of claim 16 wherein said encryption key information comprises a public key uniquely associated with said first switch.

18. (Previously Presented) The method of claim 10 wherein said third-type derivative is specific to both said second switch and said first switch.

19. (Original) The method of claim 18 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

20. (Original) The method of claim 19 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority being the manufacturer of either said first switch or said second switch.

21. (Original) The method of claim 10 wherein the step, at said second switch, of comparing said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch, comprises the sub-steps of:

reversing said third-type derivative of said defined information concerning said first switch yielding a reversed third-type derivative; and

comparing said reversed third-type derivative with said defined information concerning said first switch.

22. (Previously Presented) The method of claim 20 wherein said step of reversing said third-type derivative is performed using a public key uniquely associated with an encryption key authority, said encryption key authority specific to said first switch and said second switch.

23. (Currently Amended) A method of mutually authenticating a first port on a first switch with a second port on a second switch, the method comprising the steps of:

sending from said first port to said second port, an authentication request command having a payload of a first fact;

sending from said second port to said first port, a request acknowledge command having a payload of

a second fact,

a second-type derivative of said first fact,

defined information concerning said second switch,

and a third-type derivative of defined information concerning said second switch, the third-type derivative of defined information concerning said second switch being generated by the second switch; and

sending from said first port to said second port, a confirm authentication command having a payload of

a first-type derivative of said second fact,

defined information concerning said first switch, and

a third-type derivative of defined information concerning said first switch, the third-type derivative of defined information concerning said first switch being generated by the first switch.

24. (Previously Presented) The method of claim 23 wherein said first fact is a random number.

25. (Previously Presented) The method of claim 23 wherein said first fact is a nonce.

26. (Previously Presented) The method of claim 23 wherein said second-type derivative of said first fact is created by a method comprising the sub-steps of:

encoding said first fact to yield an encoded first fact; and

encrypting said encoded first fact.

27. (Previously Presented) The method of claim 26 wherein said encoding is performed by applying a hash function.

28. (Previously Presented) The method of claim 26 wherein said encrypting is performed using a private key unique to said second switch.

29. (Previously Presented) The method of claim 23 wherein said defined information concerning said first switch comprises encryption key information.

30. (Previously Presented) The method of claim 29 wherein said encryption key information comprises a public key uniquely associated with said first switch.

31. (Previously Presented) The method of claim 23 wherein said third-type derivative is specific to both said second switch and said first switch.

32. (Previously Presented) The method of claim 31 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

33. (Previously Presented) The method of claim 31 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority being the manufacturer of either said first switch or said second switch.

34. (Previously Presented) The method of claim 23 further comprising the step of comparing, at said second switch, said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch.

35. (Previously Presented) The method of claim 34 wherein said comparing step comprises the sub-steps of:

reversing said third-type derivative of said defined information concerning said first switch yielding a reversed third-type derivative; and

comparing said reversed third-type derivative with said defined information concerning said first switch.

36. (Previously Presented) The method of claim 35 wherein said step of reversing said third-type derivative is performed using a public key uniquely associated with an encryption key authority, said encryption key authority specific to said first switch and said second switch.

37. (Currently Amended) A method of mutually authenticating a first port on a first switch with a second port on a second switch, the method comprising the steps of:

sending from said first port to said second port, an authentication request command having a payload of

a first fact,

defined information concerning said first switch, and

a third-type derivative of defined information concerning said first switch, the third-type derivative of defined information concerning said first switch being generated by the first switch,

sending from said second port to said first port, a request acknowledge command having a payload of

a second fact,

a second-type derivative of said first fact,

defined information concerning said second switch, and

a third-type derivative of defined information concerning said second switch, the third-type derivative of defined information concerning said second switch being generated by the second switch; and

sending from said first port to said second port, a confirm authentication command having a payload of a first-type derivative of said second fact.

38. (Previously Presented) The method of claim 37 wherein said first fact is a random number.

39. (Previously Presented) The method of claim 37 wherein said first fact is a nonce.

40. (Previously Presented) The method of claim 37 wherein said second-type derivative of said first fact is created by a method comprising the sub-steps of:

encoding said first fact to yield an encoded first fact;

encrypting said encoded first fact.

41. (Previously Presented) The method of claim 40 wherein said encoding is performed by applying a hash function.

42. (Previously Presented) The method of claim 40 wherein said encrypting is performed using a private key unique to said second switch.

43. (Previously Presented) The method of claim 37 wherein said defined information concerning said first switch comprises encryption key information.

44. (Previously Presented) The method of claim 43 wherein said encryption key information comprises a public key uniquely specific to said first switch.

45. (Previously Presented) The method of claim 37 wherein said third-type derivative is associated with both said second switch and said first switch.

46. (Previously Presented) The method of claim 45 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority specific to said first switch and said second switch.

47. (Previously Presented) The method of claim 37 further comprising the step of comparing, at said second switch, said defined information concerning said first switch with said third-type derivative of said defined information concerning said first switch.

48. (Previously Presented) The method of claim 47 wherein said comparing step comprises the sub-steps of:

reversing said third-type derivative of said defined information concerning said first switch yielding a reversed third-type derivative; and

comparing said reversed third-type derivative with said defined information concerning said first switch.

49. (Previously Presented) The method of claim 48 wherein said step of reversing said third-type derivative is performed using a public key uniquely associated with an encryption key authority, said encryption key authority associated with said first switch and said second switch.

50. (Currently Amended) A method of mutually authenticating a first port on a first switch with a second port on a second switch, the method comprising the steps of:

receiving on said second port any recognized communication and interpreting said recognized communication as having a recognized purpose and an additional purpose, said additional purpose being a request for authentication command;

at said second switch, creating a second-type derivative of said recognized communication and storing said second-type derivative and said recognized communication in a memory;

sending from said second port to said first port an acknowledge request command having a payload of

a second fact,

said second type derivative of said recognized communication;

defined information concerning said second switch, and

a third-type derivative of defined information concerning said second switch, the third-type derivative of defined information concerning said second switch being generated by the second switch; and

sending from said first port to said second port, a first-type derivative of said second fact, defined information concerning said first switch, and a third-type derivative of defined information concerning said first switch, the third-type derivative of defined information concerning said first switch being generated by the first switch.

51–53. (Cancelled)